Chapter 2.4
Hazard Analysis

1. Applicability of this chapter

You are required to follow this chapter if you:

a. Do job hazard analyses or hazard analyses.

b. Are a project manager, Contracting Officer, JSC's Center Director, or the Director, Safety and Mission Assurance, Paragraph 17 of this chapter lists your responsibilities.

2. Description of Sub-element 2.4

JSC shall routinely examine and analyze safety and health hazards associated with individual jobs, processes, or phases and include results in training and hazard control programs described in Chapter 3.2 of this Handbook. This may include job hazard analysis, hardware or facility hazard analysis, or process hazard review.

3. What this chapter covers

This chapter gives you basic requirements for doing job hazard analyses and other hazard analyses and for managing risk for ground-based jobs and systems. See space shuttle or space station requirements for more information on space systems.

NOTE: Your hazard analysis may also include the required environmental impact assessment to make sure all environmental aspects have been considered and the impacts are controlled. The assessment is required by JSC's Environmental Management System to assess JSC's activities, products, or services that have effects on the environment – both positive and negative. It shall follow JPR 8553.1, "JSC Environmental Management System Manual."

4. Job hazard analysis

The following requirements apply:

a. You shall do a job hazard analysis for any job you believe to be hazardous. In this chapter, "job" means a task that someone does, not his or her position.

b. Before each hazardous operation, you shall assess any unique hazards and controls and affirm the appropriateness of the work-authorizing document. If the existing work-authorizing document is insufficient to adequately control the hazards, you shall:

   1. Assess the hazards using a Safe Plan of Action (see JSC 17773) or equivalent assessment.

   2. Include any necessary controls in the work effort. The job hazard analysis will be made available if necessary.

3. Return a copy of the completed assessment to the work authorizing document's originator to determine whether the document should be updated.

c. You shall review your job hazard analysis yearly or when the job changes.

d. Job hazard analysis shall follow Appendix G of JSC 17773, "Preparing Hazard Analyses for JSC Ground Operations." Appendix G of JSC 17773 follows the format and methodology of OSHA pamphlet 3071, "Job Hazard Analysis."

Hazard analysis and system safety

5. When a hazard analysis is required

A hazard analysis is an organized method for identifying hazards and hazard controls in a system at any point in its life cycle. JSC 17773 gives you more details on how to recognize and analyze hazards. You shall start planning for and doing hazard analyses and environmental impact assessments in the early design phases for any of the following systems and operations:

a. Aircraft systems.

b. Facilities and hazardous facility systems such as test or oxygen systems.

c. Support equipment such as test, maintenance, or training equipment.

d. Software for any of the above systems.

e. Prototypes of any of the above systems.

f. Other systems or operations when required by other chapters of this Handbook.

g. Operations and support activities, such as:

1. Constructing facilities and making hardware.
2. Experimenting on and testing systems.
3. Storing, packing, or transporting systems.
4. Checking out and using systems.
5. Maintaining or modifying systems.
6. Retrieving, disassembling, or disposing of systems.

6. Basic elements of a system safety program

A system safety program may be simple or complex, depending on the project. You shall follow these steps and may tailor them to your project:

a. Start with a preliminary hazard analysis on each proposed concept.

b. Use the preliminary hazard analysis to:

1. Document the hazards of each design concept or operation you are considering.
2. Review lessons learned from past experience.

3. Define safety and health requirements for the project.
4. Help you select which design concepts or operations to choose.
5. Plan future safety and health efforts. These could include what other hazard analyses and system safety techniques are necessary, such as subsystem hazard analyses, operation and support hazard analyses, fault-tree analyses, and hazard operability studies.

c. Use hazard analyses to support trade-off studies of different design and operational concepts during each phase of the project.

d. Trace all pertinent details of the hazard analysis and review from the initial identification of the hazard through its resolution and any updates. Use the continuous risk management approach.

e. Decide which hazard controls to use. Eliminate hazards with design measures as much as possible. Use other controls for those you can't eliminate by design.

f. Analyze your system's proposed operation for hazards. Consider all phases of your system's operation such as test, startup, operation, maintenance, and disposal.

g. Decide what risk is acceptable to your project.

h. Assess and accept the risks of the system or its operation after you have controlled the hazards by:

1. Using the most effective hazard controls that will be cost effective and won't prevent the system's mission from being accomplished.
2. Looking at the risk each hazard poses and deciding whether it's acceptable or whether you should do more to control it and lower the risk.

i. Have the right level of management accept risks.

j. Document all risk decisions and their rationale.

k. Send copies of safety analysis reports and hazard analyses to NASA Headquarters as requested.

l. Also see paragraphs 2.3 and 2.4 of NPR 8715.3, "NASA General Safety Program Requirements," for more information on the flow of a system safety program.

7. What hazard analyses contains

Your hazard analysis shall contain at least the following information:

a. The system's name and location.

b. The hazards of the system and their causes. Include hazards from human factors as well. You shall also consider hazards of interfaces between systems, and interfaces between the equipment and the facility.

c. The consequence of each hazard if it were to cause a mishap. For example, death, major injury, minor injury, or estimated property damage and dollar amount.

d. Any existing engineering or administrative controls for each hazard.

e. Proposed engineering or administrative controls for each hazard, if the existing controls are inadequate.

f. Verification methods for each control to explain how the presence of each control will be confirmed (e.g., review of procedures, inspections, etc.).

g. What would happen if the engineering or administrative controls were to fail.

h. A qualitative evaluation of the possible safety and health effects before and after the controls are in place.

i. Who was on the team that did the hazard analysis.

j. When was the last time you analyzed the system.

k. A qualitative evaluation of the risk before and after the hazard controls are in place. This is the risk that management will have to accept.

8. Assessing risk

You shall use the risk assessment code (RAC) matrix below to assess the risk of each hazard. To use this matrix:

a. Find the "consequence" or the worst-case outcome of a mishap from the hazard along the left side of the matrix. The possible consequences are:

1. Class I – Catastrophic. A condition that may cause death or permanently disabling injury, facility destruction on the ground, or loss of crew, major systems, or vehicle during the mission; schedule slippage causing launch window to be missed; cost overrun greater than 50% of planned cost.

2. Class II – Critical. A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware; schedule slippage causing launch date to be missed; cost overrun between 15% and not exceeding 50% of planned cost.

3. Class III – Moderate. A condition that may cause minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware; internal schedule slip that does not impact launch date; cost overrun between 2% and not exceeding 15% of planned cost.

4. Class IV – Negligible. A condition that could cause the need for minor first-aid treatment but would not adversely affect personal safety or health; damage to facilities, equipment, or flight hardware more than normal wear and tear level; internal schedule slip that does not impact internal development milestones; cost overrun less than 2% of planned cost.

b. Find the "likelihood" that you expect the mishap to occur across the top of the matrix. The possible likelihood estimates are:

1. Likelihood A. Likely to occur (e.g., probability > 0.1).

2. Likelihood B. Probably will occur (e.g., 0.1 ≥ probability > 0.01).
3. Likelihood C. May occur (e.g., 0.01 ≥ probability > 0.001).
4. Likelihood D. Unlikely to occur (e.g., 0.001 ≥ probability > 0.000001).
5. Likelihood E. Improbable (e.g., 0.000001 ≥ probability).

c. Find the RAC in the box where the "consequence" and "likelihood" cross.

	LIKELIHOOD ESTIMATE				
CONSEQUENCE CLASS	**A**	**B**	**C**	**D**	**E**
I	1	1	2	3	4
II	1	2	3	4	5
III	2	3	4	5	6
IV	3	4	5	6	7

9. What each RAC means

The table below tells you what action to take for each RAC. For systems in design, you shall eliminate or control the hazard before the system goes into operation. For existing systems, investigate and abate the hazard as described in Chapters 3.2 and 3.5 of this Handbook.

If the RAC is . . .	***Then the risk is . . .***
1	Unacceptable – All operations shall cease immediately until the hazard is corrected, or until temporary controls are in place and permanent controls are in work. A safety or health professional shall stay at the scene at least until temporary controls are in place. RAC 1 hazards have the highest priority for hazard controls.
2	Undesirable – All operations shall cease immediately until the hazard is corrected or until temporary controls are in place and permanent controls are in work. RAC 2 hazards are next in priority after RAC 1 hazards for control. Program Manager (directorate level), Organizational Director, or equivalent management is authorized to accept the risk with adequate justification
3	Acceptable with controls – Division Chief or equivalent management is authorized to accept the risk with adequate justification
4–7	Acceptable with controls – Branch Chief or equivalent management is authorized to accept the risk with adequate justification

10. Controlling hazards

You shall use these steps to decide what corrective action to take for any hazard found during your analysis. Take the following actions in the order below to control a hazard. Go to the next step only if the present step or previous steps aren't feasible or are too costly:

a. Change the design to eliminate or reduce the hazard. For example, use a less hazardous material or lower voltage if you can.

b. Install safety devices or guards. For example, use safety interlocks, machine guards, or relief valves if you can.

c. Install caution and warning devices. For example, use oxygen monitors or alarms if you can.

d. Use administrative controls, such as special work procedures, training, administrative barriers, and signs.

e. Use personal protective equipment.

f. Accept the risk as described in subparagraphs 6.h and 6.i of this chapter.

g. Make sure that all hazards are controlled. To do this, you shall track each hazard and keep it "open" until one of the above actions has occurred.

System safety plan and reviews

11. System safety plan

As a project manager, you shall develop a system safety program plan that describes your system safety effort. You may combine this with a safety and health plan, if possible. Use Attachment 2.4A, Appendix 2B, as a guide. The plan shall:

a. Be done before the project begins.

b. Describe engineering and management tasks for system safety.

c. Tailor the system safety program to the project based on the project's complexity, cost, criticality, or management structure.

d. Allow for free communications among all persons and organizations working on the project.

e. Be updated as the design matures.

f. Include budgets, responsibilities, and applicable safety and health requirements.

g. Include a system safety task schedule that supports the project schedule.

12. Safety reviews

As a project manager, you need to have a safety review either before or as a part of each project review. Project reviews may include preliminary design reviews or 30% design review, operational readiness inspections, etc. Safety reviews shall:

a. Status your system safety program.

b. Review hazards found before the review and prioritize them by risk.

c. Review other system safety products such as safety assessment reports.

d. Decide whether you should change the design, study other options, or do more hazard analysis.

Other requirements and responsibilities

13. Maintaining a hazard analysis or job hazard analysis

You shall:

a. Keep the analysis and review it at least every 5 years while the project is active or before making any changes to the hardware, software, or operation. This will allow you to see how valid your analysis was after you have had some experience with the system.

b. Review job hazard analyses every year or when the job changes.

14. Changes to the job, system, or operation

If you intend to change your job, system, or operation, including changes to process or chemicals used in a process, you shall:

a. Hold a safety review, update the existing hazard analysis, or do a new hazard analysis to make sure that the change doesn't create a hazard.

b. Analyze any change proposed to correct a hazard to see whether it will effectively control the hazard.

c. Include in the hazard analysis a listing of chemicals used in the process. Update the hazard analysis whenever quantities increase or processes change.

15. Other requirements for job hazard and hazard analyses

In addition to this chapter, you shall follow the requirements in these documents.

For . . .	*Follow this standard . . .*
Job hazard and hazard analyses on JSC ground-based systems	JSC 17773 NPR 8715.3, Chapter 2 NASA STD 8719.7, "Facility System Safety Guidebook"
Software safety	NASA STD-8719.13, "Software Safety"
Failure tolerance requirements for safety-critical functions	Paragraph 1.7 of NPR 8715.3
Product safety	29 CFR 1960.34(b)
Ground-based chemical processes	29 CFR 1910.119
Environmental impact assessments of new or different activities, products, or services	JPR 8553.1, "JSC Environmental Management System Manual"

16. For more information on job hazard and hazard analyses

You can find more information on job hazard and hazard analyses in these documents:

a. Chapter 2 and Appendix F of NPR 8715.3, "NASA General Safety Program Requirements," current version.

b. Langley Research Center Handbook 1740.4, "Facility System Safety Analysis and Configuration Management," current version.

c. NPR 8820.2, "Facility Project Implementation Guide," current version.

d. MIL-STD-882, "System Safety Program Requirements," current version.

17. Responsibilities

Responsibilities for hazard analysis and job hazard analysis are as follows:

a. The ***Center Director*** has the final authority for all system safety products and risk management decisions for systems and facilities at JSC and JSC field sites. He or she is responsible for appointing a senior manager at JSC and each field site to serve as the site manager for risk management decisions involving JSC personnel, property, and operations.

b. A ***project manager*** for any new or modified system, facility, or operation at JSC or a JSC field site is responsible for:

   1. Developing a system safety program for your project early in the planning phase.
   2. Making sure everyone on the project follows your system safety program.
   3. Approving a safety management plan and any system safety program plans that may be required.

4. Reporting hazards that could result in death, major injury, or major property damage to anyone or anything outside the project and other hazards, as required, to higher management.
5. Fulfilling the responsibilities in paragraphs 2.5, 2.6, 2.7, and 2.8 of NPR 8715.3.

c. The ***Director, Safety and Mission Assurance Directorate,*** is responsible for providing personnel to:

1. Providing guidance to JSC organizations on system safety programs, job hazards, and hazard analyses. Reviews programs and analyses.
2. Making sure system safety products are complete and accurate and management is properly accepting risk and documenting its decisions.
3. Supporting project and safety reviews to make sure the system safety program is being followed.
4. Fulfilling the responsibilities in paragraphs 2.5, 2.6, 2.7, and 2.8 of NPR 8715.3.

d. The ***Occupational Health Branch*** is responsible for helping JSC organizations conduct job hazard or hazard analyses for potential occupational health hazards in the workplace.

18. Safety and health records

The following organizational-level records document hazard analysis:

a. Organizational-level records:

1. Line managers and employees shall keep current copies of job hazard analyses.
2. Ground programs shall keep copies of system safety plans and hazards.

b. Center-level records – Records on environmental impact assessments are maintained in the Environmental Management System Control plan as described in JPR 8553.1, “JSC Environmental Management System Manual.”